TMA Privacy Office Information Paper

Records Management • FOIA • DUAs • HIPAA Compliance • ADP Security • Privacy Act • System of Records • PIAs

Transmission Security

HIPAA Security • November 2003

Standard Requirement

Covered entities must address transmission security as part of their technical safeguards. The Security Rule defines it as "technical security mechanisms to guard against unauthorized access to electronic protected health information (EPHI) that is being transmitted over an electronic communications network." This standard requires covered entities to assess and install appropriate technical controls to mitigate threats to data security in transit over all types of networks including but not limited to the Internet, corporate intranets, dedicated lease lines and dial-up connections.

Implementation Specifications

The standard has two implementation specifications, both of which are addressable:

- integrity controls, and
- encryption.

The first implementation specification, integrity controls, includes "security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of." Because this requirement is "addressable", compliance depends on the outcome of a covered entity's risk assessment. Integrity refers to the assurance that a transmitted message arrives at its destination exactly as it left its origin. Data often face increased threat of unauthorized modification during transmission because the entity does not always have control over the transmitting network(s). Most viruses arrive via the Internet presenting another threat to the integrity of data already present in the information system. Covered entities should determine the need for, and type of integrity controls during their organizational risk analyses. Covered entities should also describe and justify their approach to this issue in their risk management plan.

The second implementation specification, encryption, focuses on "mechanisms to encrypt electronic protected health information whenever deemed appropriate." Because this implementation standard is "addressable", compliance depends on the outcome of a covered entity's risk assessment. This is the second time that

TMA Privacy Office Information Paper

Records Management • FOIA • DUAs • HIPAA Compliance • ADP Security • Privacy Act • System of Records • PIAs

Transmission Security

encryption appears in the final rule. In this provision "encryption" appears under the "Transmission Security" standard. Encryption functions as a means of protecting the confidentiality and integrity of a message during transmission over a network or other electronic means. If other means cannot effectively protect the data against unauthorized disclosure or modification in the network environment, covered entities should implement encryption as appropriate. This determination should be based on the results of an organization's risk analysis and explained in its risk management plan. The rule sets no minimum encryption standard. While it "encourages" consideration of encryption, DHHS has advised only that EPHI must be "protected in a manner commensurate with the associated risk" when it is transmitted from one place to another. (Final Rule, p.8356 and p. 8357) Organizations can expect technological changes to shift both the cost-effectiveness of encryption technologies as well as the risk factors for interception of unencrypted transmissions.

See also:
45 CFR 164.312(e)(1)

Federal and DoD regulations that support this standard
DoD 8510.1-M
DoDD 8500.1